BitBlaze – A Binary Centric Approach to Computer Security
D. Brumley, J. Caballero, C. Hartwig, M. Kang, J. Newsome, P Poosankam, P Saxena, D. Song, H. Yin

Goal

• To develop a novel, robust binary analysis platform.
• To solve a wide spectrum of computer security via binary analysis.
  ➢ Novel attack detection, vulnerability diagnosis and worm defense.
  ➢ Comprehensive framework for malware analysis and detection.

The BitBlaze Platform

• Vine: Static Analysis Component
• Temu: Dynamic Analysis Component
• Rudder: Mixed Symbolic & Concrete Execution Engine

Worm Defense

• Worm Characteristics
  ➢ Exploit vulnerabilities
  ➢ Fast Propagation
    ❖ Affect 90% victim in < 10 minutes
• Sting
  ➢ Detection: Dynamic Taint Analysis
  ➢ Diagnosis: Static Analysis
• Signature Generation
  ➢ Fast, Accurate, Defeats Polymorphism

Malware Analysis

• Problem: Malware, Bots, Spyware
  ➢ Botnet Phenomenon [2006]
    ❖ 6 Million infections in 3 months.
    ❖ 61% US computers infected.
• BitScope - A Unified, Whole System Analysis
  ➢ Dynamic Fine-Grained Analysis
  ➢ Mixed Symbolic Execution

Other Projects

• Protocol Format Extraction
• Application Dialog Replay
• Automatic Deviation Detection

Impact

• Works robustly on Windows and Linux binaries
• Over 12 research papers: CCS, S&P, Usenix Security, NDSS, CSF, and others
  ➢ Best Paper Award at Usenix Security 2007

NSF Cyber Trust Principal Investigators Meeting
March 16-18, 2008
New Haven, CT